Revealing of Location in IP Mobility Networks

László Zömbik

Cellular telecommunication networks provide the location freedom of communication within their coverage area. In order to achieve similar freedom in IP based communication several IP mobility protocols are developed.

However, cellular networks give not only position freedom, but they provide it in a secure way. They guarantee that communication remains secret and sound, the communicating peers are mutually authenticated. Furthermore, network providers share no information about the current position of their users to unauthorised parties. Besides, those systems are designed so that no such information could be leaked. Therefore the privacy of the location is ensured.

In IP mobility, there is enormous research activity to ensure secure communication. Thus, several solutions are designed. They mainly concentrate on solving issues, which are raised, when a user intends to log in to a mobile access network. Such issues are the authentication, authorisation, and accounting or exchange of keys for later communication. They give solutions how the mobility related signalling and the user data should be protected. As well as the secure transport of the set of information, needed for handover procedure (the so-called mobile context) is also considered. Furthermore they try to utilise the features of the different kind of lower layers to achieve security efficiently.

However, none of the solutions deals with the location privacy issue.

Until the appearance of mobile IP protocols, the host IP address had been identified unambiguously the position of the host in the network. Since the number of mobile nodes still infinitesimal, the Internet community has been less interested to hide the position of a host, thus they has been concentrated just on the confidentiality of the communication.

Unfortunately, encrypted channels do not provide guarantees to location privacy, since even if the contents of the messages cannot be interpreted, the traffic shape can carry additional information for the attacker.

The aim of this presentation is to draw attention to the location privacy issues in Internet environment. As the IP based mobile communication starts to spread through the users, the need for location privacy starts to grow.

In this presentation location revealing attack is introduced, without looking into the communication itself. Based on traffic shape, different investigations (pattern matching, adaptive filtering) are performed. The efficiency and the limits of this attack are presented, as well as some effective countermeasures against it.